PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-258790

(43)Date of publication of application : 12.09.2003

---

(51)Int.Cl. H04L 9/16
G06K 17/00
H04L 9/08
H04L 12/28

---

(21)Application number : 2002-057314 (71)Applicant : CANON INC

(22)Date of filing : 04.03.2002 (72)Inventor : HAMADA MASASHI

---

(54) RADIO COMMUNICATION SYSTEM AND CONTROL METHOD THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To independently update an encryption key by a system.
SOLUTION: An access point 100 periodically broadcasts and transmits a beacon frame to the terminal of a service set. The beacon frame is equipped with a field for reporting a key number. Then, an IC card for storing the key information of a key itself in the order of key numbers is mounted at the access point and on the terminal. The access point periodically changes the key and a changed key number is distributed to the terminal by the beacon frame. Each terminal specifies the key information from the key number in the beacon frame and utilizes that key information for encryption and decryption.

LEGAL STATUS [Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] A storage means to be the radio communications system which connects a terminal and an access point by radio, to prepare for each of said terminal and access point, and to memorize an encryption key identifiable with an index, In a distribution means to distribute the index of the encryption key determined as what is used in said access point to said terminal, and said terminal The radio communications system which reads the encryption key identified by the index distributed from said access point from said storage means, and is characterized by having a means to register as an encryption key to be used.

[Claim 2] Said storage means is a radio communications system according to claim 1 characterized by including the storage which can be detached and attached freely to said terminal and access point.

[Claim 3] The radio communications system according to claim 1 or 2 characterized by newly determining the encryption key used whenever the amount of data which

communicates between said access points and terminals reaches constant value in said access point.

[Claim 4] The radio communications system according to claim 1 or 2 characterized by newly determining the encryption key used in said access point whenever it carries out fixed time amount progress.

[Claim 5] The radio control unit carry out having a storage means are the radio control unit connected with the terminal by radio, and memorize an encryption key identifiable with an index, a key decision means determine the encryption key use it, a means register as an encryption key which uses for the determined encryption key, reading from said storage means, and a distribution means distribute said determined index of an encryption key to said terminal as the description.

[Claim 6] Said storage means is a radio control unit according to claim 5 characterized by including the storage which can be detached and attached freely.

[Claim 7] Said key decision means is a radio control unit according to claim 5 or 6 characterized by newly determining the encryption key used whenever the amount of data which communicates between said terminals reaches constant value.

[Claim 8] Said key decision means is a radio control unit according to claim 5 or 6 characterized by newly determining the encryption key used whenever it carries out fixed time amount progress.

[Claim 9] The terminal unit characterized by having a means to be the terminal unit connected with the radio control unit by radio, to read the encryption key identified by storage means to memorize an encryption key identifiable with an index, and the index distributed from said radio control unit from said storage means, and to register as an encryption key to be used.

[Claim 10] Said storage means is a terminal unit according to claim 9 characterized by including the storage which can be detached and attached freely.

[Claim 11] The computer program for reading the encryption key determined as a key decision means to by_which the computer connected with the terminal by radio determines the encryption key to be used from a storage means memorize an encryption key identifiable with an index, and realizing a means register as an encryption key to be used, and a distribution means distribute said determined index of an encryption key to said terminal.

[Claim 12] Said key decision means is a computer program according to claim 11 characterized by newly determining the encryption key used whenever the amount of data which communicates between said terminals reaches constant value.

[Claim 13] Said key decision means is a computer program according to claim 11 characterized by newly determining the encryption key used whenever it carries out fixed time amount progress.

[Claim 14] The computer program for reading the encryption key identified by the index distributed from said radio control unit by computer connected with the radio

control unit by radio from a storage means to memorize an encryption key identifiable with an index, and realizing a means to register as an encryption key to be used.

[Claim 15] It is the control approach of the radio communications system which connects a terminal and an access point by radio. The index of the encryption key determined as what is used in said access point is read from a storage means to memorize an encryption key identifiable with an index. In the distribution process which distributes the index of the encryption key determined as the process registered as an encryption key to be used, and the thing to use in said access point to said terminal, and said terminal The control approach of the radio communications system which reads the encryption key identified by the index distributed from said access point from a storage means to memorize an encryption key identifiable with an index, and is characterized by having the process registered as an encryption key to be used.

[Claim 16] The radio communications system which is a radio communications system including the access point connected to the wire net, and is characterized by to have the storage with which said client terminal and the device of the both sides of said access point were equipped, a means match the key information for data encryption with an in DEKKUSSU number, and memorize it in said storage, and a means return the key information for said encryption from said storage corresponding to the inquiry by said in DEKKUSSU number from said device side.

[Claim 17] The radio communications system according to claim 16 characterized by having further an encryption means to encipher commo data using the key for said encryption read from said storage.

[Claim 18] Said encryption means is a radio communications system according to claim 17 characterized by considering as the object of encryption of all the data on a communication link frame.

[Claim 19] Said encryption means is a radio communications system according to claim 17 characterized by considering as the object of encryption of the data except the management data on a communication link frame.

[Claim 20] Said access point is a radio communications system given in claim 16 which the access point concerned carries out broadcast transmission of the beacon frame to which the index number of the encryption key information under current use was added with a fixed time interval, and is characterized by notifying the profile information of the area which said access point generalizes to said client terminal thru/or any 1 term of 19.

[Claim 21] It is the radio communications system according to claim 17 to 20 characterized by enciphering the data which have a means by which said access point changes said key information at intervals of predetermined within the limits of said number for in DEKKUSSU in said wireless local communication network, read the key information for said encryption corresponding to a random number from said

removable storage, and are transmitted from said access point using the encryption key information concerned.

[Claim 22] Said access point is the radio communications system according to claim 21 carry out changing the encryption key which has a means measure the encryption amount of data used for the local communication link between the access point-client terminals concerned, and a means check the existence of a local communication link, performs modification processing of after termination of a local communication link of 1 communication-link frame unit and an encryption key whenever it exceeded the amount as which said encryption amount of data was specified, and uses to subsequent local communication links with said means as the description.

[Claim 23] Said access point is the radio communications system according to claim 21 carry out changing the encryption key which has a means clock the communication link time amount used for the local communication link between the access point-client terminals concerned, and a means check the existence of a local communication link, performs in modification processing of after termination of a local communication link of 1 communication-link frame unit and an encryption key whenever it goes through the time amount as which said encryption communication link time amount was specified, and uses to subsequent local communication links with said means as the description.

[Claim 24] According to modification of said encryption key, said access point is a radio communications system according to claim 22 or 23 with which the index number of the encryption key notified using said beacon frame is characterized by making it follow in footsteps and change to the encryption key which said access point is using.

[Claim 25] 24 is [claim 21 characterized by having a means to add the warning information for notifying trouble generating, and to transmit on said beacon frame, and said access point notifying the purport that the key information for said encryption went wrong to said client terminal the failure case at steady modification of an encryption key at read-out, using said beacon frame from said removable storage thru/or] the radio communications system of a publication either.

[Claim 26] Said client terminal is a radio communications system according to claim 24 characterized by having the means which reads the index number of the use encryption key on the received beacon frame, and for the key information for data encryption coming to hand from said storage according to modification of the index number concerned, and performing a communication link data encryption.

[Claim 27] Said client terminal is a radio communications system according to claim 25 characterized by performing an alarm display to said terminal user when it has the means which reads the information on the purport that steady modification of encryption on the received beacon frame went wrong, and a means to perform an alarm display to the client terminal user concerned and said failure is detected.

[Claim 28] The radio communications system according to claim 16 to 27 characterized by a radio medium being wireless LAN.
[Claim 29] The radio communications system according to claim 16 to 27 characterized by a radio medium being the enclosure of PHS.
[Claim 30] The radio communications system according to claim 16 to 27 characterized by a radio medium being Bluetooth.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the radio communications system which strengthens the security to a radio wire-tapping person using autonomous modification of the encryption key especially used for a communication link data encryption, and its control approach in the local communication network which used for example, the radio medium about the communication system and the encryption approach of performing an encryption communication link.
[0002]
[Description of the Prior Art] There are a thing of the independent method which consists of only wireless terminals by which peer to peer connection was made, and a thing of the infrastructure method which constitutes a service area (basic service set) from one access point and a wireless terminal, and is constituted by making cable connection of two or more access points, and connecting in wireless local communication system, such as the conventional wireless LAN system. The system by the latter method is equipped with the access point which has a radio function for connecting with Cable LAN from a client terminal and client terminals, such as a personal computer equipped with the radio function. In such a system, it is wireless between client terminals and it communicates via an access point to Cable LAN. In radio, since the contents of a communication link can be monitored, it is necessary to perform an encryption communication link for informational secrecy. Therefore, the encryption key information used by the basic service set of the radio concerned must be shared in one service set. The encryption key information used by the service set was set up in the client terminal equipment which constitutes communication system, and the initialization process phase of an access point.
[0003]
[Problem(s) to be Solved by the Invention] However, an encryption communication link is monitored in the above-mentioned conventional example, and it is possible to presume the encryption key used in the communications area which wireless local

communication system monitored from the monitored encryption signal. In recent years, the throughput of information management systems, such as a personal computer, especially improves, and presuming an encryption key from the monitored encryption signal using the cheap device which generally spread can carry out now comparatively in a short time. Therefore, after the initialization process of wireless local communication system, when encryption data communication is continued using the same encryption key, without performing resetting of an encryption key, also after a wire-tapping person specifies an encryption key, the communication link will be continued using the encryption key, and the situation where the contents of the encryption communication link will be decoded by the wire-tapping person may also be produced.

[0004] In view of the above-mentioned conventional example, accomplished this invention, and it makes it possible to change autonomously the encryption key used in the wireless area which the access point concerned generalizes by initiative of an access point. By furthermore, the thing for which the cryptographic key related information transmitted through a wireless circuit is limited to an encryption key and the index information to which it was made to correspond Acquisition of an encryption key [/ in addition to the client terminal which does not have cryptographic key information] is made difficult, and it aims at offering the radio communications system which raised information safety, and its control approach.

[0005] Furthermore, the terminal which permits access, and the terminal which does not permit access can be visually identified by storing correlation with encryption key information and an index number in a removable storage, and it aims at offering the radio communications system which raised information safety, and its control approach.

[0006]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, this invention consists of the following configurations.

[0007] A storage means to be the radio communications system which connects a terminal and an access point by radio, to prepare for each of said terminal and access point, and to memorize an encryption key identifiable with an index, In a distribution means to distribute the index of the encryption key determined as what is used in said access point to said terminal, and said terminal The encryption key identified by the index distributed from said access point is read from said storage means, and it has a means to register as an encryption key to be used.

[0008] Said storage means contains still more preferably the storage which can be detached and attached freely to said terminal and access point.

[0009] The encryption key used whenever the amount of data which communicates between said access points and terminals reaches constant value in said access point still more preferably is newly determined.

[0010] Still more preferably, whenever it carries out fixed time amount progress in said access point, the encryption key to be used is newly determined.
[0011] Or other side faces of this invention consist of the following configurations.
[0012] It has a storage means are the radio control unit connected with the terminal by radio, and memorize an encryption key identifiable with an index, a key decision means determine the encryption key to be used, a means register as an encryption key used for the determined encryption key, reading from said storage means, and a distribution means distribute said determined index of an encryption key to said terminal.
[0013] Said storage means contains still more preferably the storage which can be detached and attached freely.
[0014] Said key decision means newly determines still more preferably the encryption key used whenever the amount of data which communicates between said terminals reaches constant value.
[0015] Said key decision means newly determines still more preferably the encryption key used whenever it carries out fixed time amount progress.
[0016] Or other side faces of this invention consist of the following configurations.
[0017] It is the terminal unit connected with the radio control unit by radio, and the encryption key identified by storage means to memorize an encryption key identifiable with an index, and the index distributed from said radio control unit is read from said storage means, and it has a means to register as an encryption key to be used.
[0018] Or other side faces of this invention consist of the following configurations.
[0019] It is a radio communications system including the access point connected to the wire net, and has the storage with which said client terminal and the device of the both sides of said access point were equipped, a means to match the key information for data encryption with an in DEKKUSSU number, and to memorize it in said storage, and a means to return the key information for said encryption from said storage corresponding to the inquiry by said in DEKKUSSU number from said device side.
[0020]
[Embodiment of the Invention] It explains below [the first operation gestalt], referring to an attached document about the gestalt of operation of the encryption system of the wireless local communication link concerning this invention.
[0021] In the encryption system of the wireless local communication link in this operation gestalt, whenever it makes wireless LAN (ISO8802.11 conformity system) into wireless local communication media, it uses the infrastructure mode of wireless LAN, using an IC card as a removable storage and the communication link of the data of the amount of conventions is performed on a radio medium, the key for encryption used by the wireless medium is changed automatically.
[0022] Drawing 1 is a LAN structure-of-a-system conceptual diagram containing the wireless local communication system in this operation gestalt. Drawing 1 shows the

condition of not performing data communication. The whole LAN system has the wire net (cable LAN) 10 which is a backbone communication network, and the wireless LAN system 11 which is a local radio network. The wireless LAN system 11 is constituted by an access point 100 and the client terminals 110, 120, and 130. The access point 100 has the function as a control unit it not only to connect Cable LAN with wireless LAN, but to report the information shared by the terminal and access point in a basic service set to each terminal of a service set.

[0023] moreover, an access point 100 and the client terminal 110,120,130 -- each -- IC cards 101, 111, 121, and 131 as a storage -- it has the removable IC card adapter for each. this IC card 101,111,121,131 -- respectively -- being alike -- it is collectively memorized by the index value to show the encryption key information used for encryption, and its encryption key information. At the time of cryptocommunication, the client terminal which performs an access point 100 and an encryption communication link is equipped with an IC card.

[0024] An access point 100 transmits intermittently the beacon frame 12 for reporting area profile information to all the client terminals that carry out a ** area into wireless area with a fixed time interval by the broadcast formula in infrastructure mode. Area profile information is information which shows the profile (assembly of setting information) of the wireless area (basic service set) which an access point 100 generalizes. With this operation gestalt, intermittent transmission is carried out including the key number (index value to show the value of a key) for the encryption (encryption according to the WEP method of ISO 8802.11) which an access point 100 is using for the area profile information transmitted by the beacon frame 12. In addition, a WEP method is the option function of ISO 8802.11, and is a method which enciphers data in a MAC layer (MAC: media access control), attaches the data for media authorization codes, and checks the existence of an error or an alteration. The key used for this encryption is called a WEP key.

[0025] Drawing 2 is the conceptual diagram showing the situation under data communication in the encryption system of the wireless local communication link in this operation gestalt. Frames 20 and 21 are encryption data communication frames by the renewal method of a dynamic WEP key used in the case of data communication. In addition, in this operation gestalt, whenever data communication of the amount of conventions is performed in area, the WEP key is updated.

[0026] The functional block diagram of the wireless LAN function part of the wireless LAN client terminal of this operation gestalt is shown in drawing 13 .

[0027] The wireless section 1301 manages transmission and reception. The baseband processing section 1302 manages the strange recovery of a signal. The MAC control section 1303 manages coding, a decryption, and timing management of data. A control section 1304 manages the control more than a frame level. The memory for work areas in RAM1305 and ROM1306 are memory which stores a control program. The IC

card interface section 1307 offers the electric mechanical interface for writing data in IC card 1309, and reading data from IC card 1309. The index value the information element of a WEP key and for each information-element selection is related with IC card 1309, and it memorizes inside (refer to drawing 6). The application interface section 1308 offers an interface with other components in the client terminal which communicates using a wireless LAN function part.

[0028] The functional block diagram of the wireless LAN access point of this operation gestalt is shown in drawing 14 .

[0029] The wireless section 1401 manages transmission and reception. The baseband processing section 1402 manages the strange recovery of a signal. The MAC control section 1403 manages coding, a decryption, and timing management of data. A control section 1404 manages the control more than a frame level. The memory for work areas in RAM1405 and ROM1406 are memory which stores a control program. The IC card interface section 1407 offers the electric mechanical interface for writing data in IC card 1409, and reading data from IC card 1409. The index value the information element of a WEP key and for each information-element selection is related with IC card 1409, and it memorizes inside (refer to drawing 6). The cable LAN interface section 1408 offers the interface of an access point and Cable LAN.

[0030] The example of a format of the beacon signal of wireless LAN (ISO8802.11 conformity system) is shown in drawing 3 . A beacon signal is a signal used in order for broadcasting to report the information on area to all client terminals from an access point in infrastructure mode. The field appointed by the MAC header 301 and time stump 302 in which it is shown that it is the frame of a media-access-control (MAC) layer, the capability information 304 grade of two octets mentioned later, and specification is defined as the format of drawing 3 .

[0031] Drawing 4 is drawing showing the contents by which the capability (capability) information 304 included in the beacon signal of drawing 3 was standardized. A bit 5 to the bit 15 is a spare bit.

[0032] The example of a format which extended the capability information 304 on the beacon signal in the wireless LAN (ISO8802.11 conformity system) of this operation gestalt to drawing 5 is shown. With this operation gestalt, it sets as a cryptographic key number 506 for the index value corresponding to a WEP key while it is 11 bits from which operation is suspended as reserve area 406 on the beacon frame signal for the capability information 304 which consists of two octets and an access point is using 6 bits of a bit 5 to the bit 10 to be well-known to the client terminal in a basic service set. 64 kinds of WEP keys can be specified by the cryptographic key number 506. Furthermore, it is determined as the warning bit 507 for notifying that the fault on the employment by the side of an access point (WEP key information cannot be read from an IC card) has produced the bit 11 of the reserve area 406. Remaining 4 bits is reserved as reserve area.

[0033] Drawing 6 shows the example of the key information registration table stored as WEP key information in the IC card, when the data length of the WEP key information on wireless LAN is 40 bits in this operation gestalt. The index value (1-64) ** table of the cryptographic key number 506 is corresponded and carried out to a WEP key, and the 40-bit actual WEP key information 601-664 is memorized by the IC card corresponding to the cryptographic key number. And the IC card has the function to return the WEP key information corresponding to the inputted index value, to the input of an index value. This function is carried out by performing the program stored in the memory in which this was also built by the processor built in the IC card.

[0034] Drawing 7 and drawing 8 are the mimetic diagrams of the logical file structure in an IC card. Among these, drawing 7 is an example which mounted ID (AID) for discernment of the most significants 700-DFs 720 by the method assigned for every service vendor. Drawing 8 is an example which mounted ID (AID) for discernment of the most significants 800-DFs 820 by the method assigned for every types of services. Anyway, it memorizes with the storage gestalt shown in the storage area in EF KEYINFO72001 and 82001 of drawing 7 and drawing 8 at drawing 6 . Therefore, an IC card can acquire and output the WEP key information corresponding to the index value which followed this logical file structure and was inputted with reference to the key information registration table, when an index value is inputted.

[0035] The modification approach of the WEP key in a <modification procedure of WEP key> wireless LAN system is explained using the sequence chart of drawing 9 , and the processing flow chart of the access point of drawing 10 and the processing flow chart of the client terminal of drawing 11 . This operation gestalt shows the example which uses that the amount of data which communicates through a wireless access point exceeded the amount of conventions as a trigger of WEP key modification. An access point 100 integrates the communication link amount of data between the client terminals in a service area using a counter etc., whenever transmission and reception of data occur, and it measures it with the amount of conventions defined beforehand. In addition, the amount of data can be performed only within data transmission or reception.

[0036] And as shown in drawing 9 , when it judges with the amount of data with which the wireless access point 100 communicates through it having exceeded the amount of conventions, the processing shown in drawing 10 is started in the wireless access point concerned.

[0037] First, the counter which counts the transmission amount of data integrated by current is cleared (1001), and the cryptographic key number (index value corresponding to a WEP key) to change is chosen by the predetermined operation (1002). How to make an index the remainder which generates the approach and random number which add 1 to the last key number for example most simply as an operation for determining an index value, and makes the 64 law etc. can be considered.

An important point is for the last key number to be made not to be chosen again. Moreover, even if it allows selection for the second time, a key number needs to be determined so that an encryption key may be changed at sufficiently short spacing to time amount required in order to presume an encryption key from a cryptocommunication sentence. The communication link amount of data (it is hereafter called the trigger amount of data) used as the trigger of key modification also needs to be determined from this viewpoint.

[0038] If a cryptographic key number is determined, an access point 100 will publish the WEP key information requirements which added the cryptographic key number to IC card 101 with which it is equipped (1003). The WEP key information response which added the WEP cryptographic key information over the specified cryptographic key number with IC card 101 which received WEP key information requirements is returned.

[0039] An access point 100 judges whether it is during current data communication a reception beam case (1004-Y) normally about a WEP cryptographic key information response (1005). If it is during data communication, queuing will be performed till termination per 1 data communication. If it is not during data communication, it will change into the WEP cryptographic key information that the encryption key (key of WEP) to be used from now on was received from said IC card, and the warning bit for alarm displays will be cleared (step 1006). And a new cryptographic key number (index value corresponding to said WEP key) and a warning bit are set, and it notifies to the capability information on a beacon frame by broadcasting to the client terminal in area (step 1007).

[0040] On the other hand, a time-out etc. is produced, and normally, when there is no reception eclipse (1004-N), the warning bit for alarm displays is set for a response (1008), a cryptographic key number (index value corresponding to said WEP key) and a warning bit value are set to the capability information on a beacon frame, and it notifies by broadcasting to the client terminal in area (step 1007). In this case, what is necessary is just to set the current value as it is, for example, since a new cryptographic key number is not obtained. In addition, what is necessary is just to set the cryptographic key number currently used as it is as cryptographic key information 506 about the beacon frame transmitted when the amount of data has not reached default value. Or it can also be shown that the cryptographic key number is not changed by displaying the purport which does not have modification of a cryptographic key, for example by the cryptographic key number 0 etc.

[0041] Next, actuation of the client terminal 110 which received the beacon frame is explained with reference to drawing 11 . In addition, actuation with any same client terminal is performed.

[0042] The client terminal 110 judges whether the warning bit is set from the received beacon frame by reading "cryptographic key number" 506 within capability

information, and "warning bit" 507 (1101) (1102). If set, the alarm display of the purport by which a key was not updated in the client terminal will be performed (1107), and one batch will be ended. On the other hand, if the warning bit is not set and modification is not detected with reference to "a cryptographic key number (1103)", one batch is ended as it is.

[0043] When modification of a "cryptographic key number" is detected (1103), to IC card 111 with which it is equipped, the client terminal 101 adds a cryptographic key number, and performs WEP key information requirements (1104). As an index value corresponding to WEP key information for the specified cryptographic key number, IC card 111 adds cryptographic key information (WEP cryptographic key information), and returns a WEP key information response.

[0044] The client terminal 101 judges a WEP key information response in a reception beam normally (1105), and if it receives normally, it will change it into the WEP cryptographic key information that the encryption key (key of WEP) to be used from now on was received from IC card 111.

[0045] On the other hand, normally, when there is no reception eclipse (1105-N), an alarm display is carried out for the WEP key information response from IC card 111 to the client terminal 101 (1107), and one batch is ended.

[0046] Actuation of the IC card connected to the access point, the client terminal, and each of a more than is shown in drawing 9 . In drawing 9 , the access point has transmitted the beacon signal periodically to the client terminal in a service set (broadcast transmission). And if the communication link amount of data after changing a WEP key finally after beacon signal 901 transmission exceeds constant value, the WEP key information requirements 903 will be published to the IC card which determined a cryptographic key number new as a WEP key modification trigger 902, and was connected in it in the access point, a cryptographic key number will be notified, and it will wait for the reception of the WEP key information response 904 to it. If the WEP key information response 904 is received, it will set up that the WEP key information included in the WEP key information response should be used making it into a new cryptographic key, the cryptographic key number newly determined as the cryptographic key number field of the beacon signal 905 will be set up, and broadcast transmission of the beacon signal 905 will be carried out. At a client terminal, if a beacon signal is received, a setup according to the signal included there will be performed, but if a cryptographic key number has modification especially, the WEP key information requirements 907 will be published to the IC card connected to the client terminal, a cryptographic key number will be notified, and it will wait for the reception of the WEP key information response 908 to it. If the WEP key information response 908 is received, a client terminal will be set up that the WEP key information included in the WEP key information response should be used making it into a new cryptographic key.

[0047] The above processing enables it to update the key for encryption (WEP cryptographic key) autonomously during network employment by making an excess of a default of the communication link amount of data on a wireless LAN medium into a trigger. For this reason, it becomes possible to raise the security to the interception of communications by third persons, such as a wireless LAN client which does not hold the IC card for a service set concerned. Moreover, the improvement in security about access to the network by the third person without authority is also attained at coincidence.

[0048] Especially distribution of the key information from an access point to each terminal is performed in the form of distribution of a cryptographic key number, and the WEP key information itself is not distributed. Therefore, in the terminal which does not hold the IC card currently used for key management in this operation gestalt, it becomes impossible to monitor distribution of the key information itself and to specify a key, and improvement in much more security can be aimed at.

[0049] Moreover, it becomes possible to change a WEP key quickly simple, the special procedure for key distribution becoming unnecessary, and securing security by including a cryptographic key number in a beacon signal, and distributing it.

[0050] Furthermore, since key information is managed with the IC card, security can be further raised by exchanging the IC card itself for the IC card holding new key information.

[0051] Furthermore, with this operation gestalt, since spacing which changes a WEP key is set up by the communication link amount of data and can be set, exchange of data can change a WEP key frequently in a frequent service set.

[0052] The example which uses for [operation gestalt of ** second] drawing 12 deadline of "the same WEP key duration timer" clocked in a wireless access point as a trigger (902 of drawing 9) of WEP key modification is shown.

[0053] When "the same WEP key duration timer" passes the deadline of in the wireless access point 100, the processing shown in drawing 12 is started in the wireless access point concerned.

[0054] First, the cryptographic key number (index value corresponding to a WEP key) which changes "the same WEP key duration timer" to current by the predetermined operation after initializing (1201) is chosen (1202). The same WEP key duration timer is realizable using the timer with which the control section 1404 of drawing 14 is equipped. Moreover, the restart of the timer is immediately carried out after initialization.

[0055] An access point 100 publishes the WEP key information requirements which added the cryptographic key number (index value corresponding to a WEP key) to IC card 101 with which it is equipped (1203 903).

[0056] IC card 100 returns the WEP key information response to the specified cryptographic key number (index value corresponding to a WEP key) which added

cryptographic key information (information on a WEP key) to an access point 100 (904).

[0057] It changes into the cryptographic key information which the access point 100 judged whether it was during current data communication a reception beam case (1204-Y) normally about a WEP key information response (1205), performed queuing till termination per 1 data communication when it was during data communication, and received the encryption key (key of WEP) to be used from now on from IC card 101 when it was not during data communication, and the warning bit for alarm displays is cleared (1206).

[0058] The key number number (index value corresponding to a WEP key), warning bit which the warning bit for alarm displays is normally set for a WEP key information response when there is no reception eclipse (1204-N) (1208), and are correspondence information on the other hand A value is set to said beacon frame and it notifies by broadcasting to the client terminal in area (905 1207).

[0059] Also in the wireless LAN system of the client terminal indicated to be the access point which performs control shown in this operation gestalt by the above processing with the 1st operation gestalt combined and boiled By making into a trigger deadline of "the same WEP key duration timer" clocked in an access point 100 It becomes possible to update the key for encryption (WEP key) autonomously during real employment, and it becomes possible to raise the communication link security to wire tapping of a third person called the wireless LAN client which does not hold the IC card for a service set concerned like the first operation gestalt.

[0060] Moreover, if same WEP key duration is made programmable, according to the improvement in the engine performance of the processor used for refinement and cryptographic key decode of the cryptographic key decode approach, security is maintainable by shortening the same WEP key duration.

[0061] Moreover, since a simple and quick WEP key can be changed by not distributing the key itself but distributing a key number, even if it sets up spacing which changes a key for a short time, the processing processing delay resulting from it can be controlled. Therefore, the frequency of key modification can be raised and the resistance over security **** can be raised.

[0062] Furthermore, with this operation gestalt, since spacing which changes a WEP key is set up by time amount and can be set, modification of the key for every fixed time amount can be guaranteed. (Other operation gestalten) In said operation gestalt, the example which changes periodically the cryptographic key for enciphering the data transmitted as a wireless medium for local radio communications systems on the radio circuit at the time of using the infrastructure mode of the wireless LAN system of 8802.ISO11 conformity was shown. However, the application to the local radio communications system PHS with which it consists of one access point and two or more clients, and the information about the wireless area concerned is regularly

reported from an access point even except the infrastructure mode of the wireless LAN system of 8802.ISO11 conformity, for example, premises, Bluetooth (Blue tooth), etc. is possible.

[0063] Moreover, in said operation gestalt, although the IC card is used as an encryption key (WEP key) information storing module, even if it uses other storage modules, such as a PC card, the same effectiveness is acquired.

[0064] Moreover, although management of a key is performed by the IC card with the above-mentioned operation gestalt, an access point and each of each client terminal may be the configurations of managing a key. In this case, security can be further raised by adding the sequence which transmits a WEP key from an access point to each terminal.

[0065] Moreover, the amount of data which serves as a trigger of WEP key modification in the 1st operation gestalt may be the amount of data set as the object of encryption, and may be the amount of data of the whole data transmitted and received.

[0066] In addition, even if it applies this invention to the system which consists of two or more devices (for example, a host computer, an interface device, a reader, a printer, etc.), it may be applied to the equipments (for example, a copying machine, facsimile apparatus, etc.) which consist of one device.

[0067] Moreover, the purpose of this invention supplies the storage (or record medium) which recorded the program code of the software which realizes the function of the operation gestalt mentioned above to a system or equipment, and is attained also by reading and performing the program code with which the computer (or CPU and MPU) of the system or equipment was stored in the storage.

[0068] In this case, the function of the operation gestalt which the program code itself read from the storage mentioned above will be realized, and the storage which memorized that program code itself and program code will constitute this invention.

[0069] Moreover, by performing the program code which the computer read, a part or all of processing that the operating system (OS) which the function of the operation gestalt mentioned above is not only realized, but is working on a computer based on directions of the program code is actual is performed, and also when the function of the operation gestalt mentioned above by the processing is realized, it is contained.

[0070] Furthermore, after the program code read from the storage is written in the memory with which the functional expansion unit connected to the functional expansion card inserted in the computer or the computer is equipped, a part or all of processing that CPU with which the functional expansion card and functional expansion unit are equipped is actual performs, and also when the function of the operation gestalt mentioned above by the processing is realized, it is contained based on directions of the program code.

[0071]

[Effect of the Invention] As explained above, according to this invention, in wireless local communication system, it becomes possible to change autonomously the encryption key used in the wireless area which the access point concerned generalizes by initiative of an access point. Moreover, since the cryptographic key related information transmitted through a wireless circuit is limited to the index information for storage access connected to the terminal, except a client terminal with a storage [finishing / the cryptographic key information storage concerned], it becomes difficult for actual encryption key information to come to hand. For this reason, it leads to improvement in the information security in the data communication in wireless local communication system.

[0072] Moreover, since correlation of encryption key information and an index number is stored in a removable storage, it becomes possible to make the access propriety of a client terminal equipment identify visually according to the wearing condition of a storage.

[0073] Furthermore, since correlation of encryption key information and an index number is stored in a removable storage, improvement in the security about access to the network by the third person without authority is attained.

[0074] Furthermore, since a cryptographic key number can be distributed without a special procedure to each terminal, it becomes possible to change a key quickly simple, securing security.

[0075] Furthermore, since it has managed with the storage which can detach and attach key information freely, security can be further raised by exchanging the storage itself for the storage holding new key information.

[0076] Furthermore, since spacing which changes a key is set up by the communication link amount of data and can be set, exchange of data can change a key frequently in a frequent service set.

[0077] Moreover, if modification of the time interval which changes a key is enabled, according to the improvement in the engine performance of the processor used for refinement and key decode of the key decode approach, security is maintainable by shortening the time interval.

[0078] Moreover, since a simple and quick key can be changed by not distributing the key itself but distributing a key number, even if it sets up spacing which changes a key for a short time, the processing processing delay resulting from it can be controlled. Therefore, the frequency of key modification can be raised and the resistance over security **** can be raised.

[0079] Furthermore, modification of the key for every fixed time amount can be guaranteed by setting up spacing which changes a key by time amount.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The cipher system structure-of-a-system conceptual diagram of the wireless local communication link in an operation gestalt

[Drawing 2] The cipher system structure-of-a-system conceptual diagram of the wireless local communication link in an operation gestalt

[Drawing 3] Drawing of the beacon frame format of an ISO8802.11 conformity system

[Drawing 4] Drawing of a beacon frame top capability information format of an ISO8802.11 conformity system

[Drawing 5] Drawing of the extended example of a format of the capability information in an operation gestalt

[Drawing 6] Drawing of the example of a WEP key information-element registration table of an operation gestalt

[Drawing 7] Drawing of the example 1 of a logical format configuration on the IC card of an operation gestalt

[Drawing 8] Drawing of the example 2 of a logical format configuration on the IC card of an operation gestalt

[Drawing 9] Drawing of the example of a modification sequence chart of the WEP key of an operation gestalt LAN system

[Drawing 10] The WEP key modification flow chart of the wireless LAN access point of the 1st operation gestalt

[Drawing 11] The WEP key modification flow chart of the wireless LAN client terminal of an operation gestalt

[Drawing 12] The WEP key modification flow chart of the wireless LAN access point of the 2nd operation gestalt

[Drawing 13] The functional block diagram of the wireless LAN client terminal of an operation gestalt

[Drawing 14] The functional block diagram of the wireless LAN access point of an operation gestalt

[Description of Notations]

10 Wire Net (Cable LAN)

11 Local Radio Network (Wireless LAN)

12 Beacon Frame

20 Data Frame Enciphered with Dynamic WEP Key

21 Data Frame Enciphered with Dynamic WEP Key

100 Access Point

101 IC Card (WEP Key Table Storing)

110 Client Terminal

111 IC Card (WEP Key Table Storing)
120 Client Terminal
121 IC Card (WEP Key Table Storing)
130 Client Terminal
131 IC Card (WEP Key Table Storing)
1301 Wireless Section
1302 Baseband Section
1303 MAC Control Section
1304 Control Section
1305 RAM
1306 ROM
1307 IC Card Interface Section
1308 Application Interface Section
1309 IC Card
1401 Wireless Section
1402 Baseband Section
1403 MAC Control Section
1404 Control Section
1405 RAM
1406 ROM
1407 IC Card Interface Section
1408 Cable LAN (Communication Network) Interface Section
1409 IC Card

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－258790
（P2003－258790A）
(43)公開日　平成15年９月12日(2003.9.12)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
H04L	9/16		G06K	17/00	L　5B058
G06K	17/00		H04L	12/28	300Z　5J104
H04L	9/08			9/00	643　5K033
	12/28	300			601E

審査請求　未請求　請求項の数30　ＯＬ　（全 14 頁）

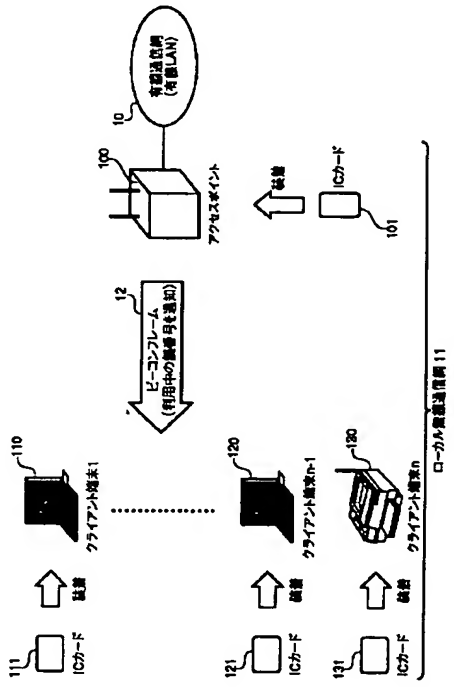
(21)出願番号　特願2002－57314(P2002－57314)
(22)出願日　平成14年３月４日(2002.3.4)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　浜田　正志
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100076428
弁理士　大塚　康徳　(外３名)

Ｆターム(参考)　5B058 CA01 KA02 KA33 YA20
5J104 AA16 JA03 PA07
5K033 AA08 CC01 DA05 DA17 DB19

(54)【発明の名称】　無線通信システムおよびその制御方法

(57)【要約】
【課題】暗号化鍵の更新をシステムにより自立的に行わせる。
【解決手段】アクセスポイント１００は、ビーコンフレームをサービスセットの端末に対して定期的に放送送信している。ビーコンフレームに、鍵番号を通知するためのフィールドを設けておく。そして、アクセスポイントと端末には、鍵そのものである鍵情報をその鍵番号順に記憶するＩＣカードが装着されている。アクセスポイントは定期的に鍵を変更し、変更した鍵番号をビーコンフレームにより端末に配信する。各端末は、ビーコンフレーム中の鍵番号からかぎ情報を特定し、それを暗号化および復号に利用する。



1

【特許請求の範囲】

【請求項１】　端末とアクセスポイントとを無線通信により接続する無線通信システムであって、
前記端末およびアクセスポイントそれぞれに備えられ、暗号化鍵を索引により識別可能に記憶する記憶手段と、
前記アクセスポイントにおいて使用するものと決定された暗号化鍵の索引を前記端末に配信する配信手段と、
前記端末において、前記アクセスポイントより配信された索引により識別される暗号化鍵を前記記憶手段より読み出して、使用する暗号化鍵として登録する手段とを備えることを特徴とする無線通信システム。

【請求項２】　前記記憶手段は、前記端末およびアクセスポイントに対して着脱自在な記憶媒体を含むことを特徴とする請求項１に記載の無線通信システム。

【請求項３】　前記アクセスポイントにおいては、前記アクセスポイントと端末との間で通信されるデータ量が一定値に達する毎に使用する暗号化鍵を新たに決定することを特徴とする請求項１または２に記載の無線通信システム。

【請求項４】　前記アクセスポイントにおいては、一定時間経過する毎に使用する暗号化鍵を新たに決定することを特徴とする請求項１または２に記載の無線通信システム。

【請求項５】　端末と無線通信により接続された無線通信制御装置であって、
暗号化鍵を索引により識別可能に記憶する記憶手段と、
使用する暗号化鍵を決定する鍵決定手段と、
決定された暗号化鍵を前記記憶手段より読み出して、使用する暗号化鍵として登録する手段と、
前記決定された暗号化鍵の索引を前記端末に配信する配信手段とを備えることを特徴とする無線通信制御装置。

【請求項６】　前記記憶手段は、着脱自在な記憶媒体を含むことを特徴とする請求項５に記載の無線通信制御装置。

【請求項７】　前記鍵決定手段は、前記端末との間で通信されるデータ量が一定値に達する毎に使用する暗号化鍵を新たに決定することを特徴とする請求項５または６に記載の無線通信制御装置。

【請求項８】　前記鍵決定手段は、一定時間経過する毎に使用する暗号化鍵を新たに決定することを特徴とする請求項５または６に記載の無線通信制御装置。

【請求項９】　無線通信制御装置と無線通信により接続された端末装置であって、
暗号化鍵を索引により識別可能に記憶する記憶手段と、
前記無線通信制御装置より配信された索引により識別される暗号化鍵を前記記憶手段より読み出して、使用する暗号化鍵として登録する手段とを備えることを特徴とする端末装置。

【請求項１０】　前記記憶手段は、着脱自在な記憶媒体を含むことを特徴とする請求項９に記載の端末装置。

2

【請求項１１】　端末と無線通信により接続されたコンピュータにより、
使用する暗号化鍵を決定する鍵決定手段と、
決定された暗号化鍵を、暗号化鍵を索引により識別可能に記憶する記憶手段より読み出して、使用する暗号化鍵として登録する手段と、
前記決定された暗号化鍵の索引を前記端末に配信する配信手段とを実現させるためのコンピュータプログラム。

【請求項１２】　前記鍵決定手段は、前記端末との間で通信されるデータ量が一定値に達する毎に使用する暗号化鍵を新たに決定することを特徴とする請求項１１に記載のコンピュータプログラム。

【請求項１３】　前記鍵決定手段は、一定時間経過する毎に使用する暗号化鍵を新たに決定することを特徴とする請求項１１に記載のコンピュータプログラム。

【請求項１４】　無線通信制御装置と無線通信により接続されたコンピュータにより、
前記無線通信制御装置より配信された索引により識別される暗号化鍵を、暗号化鍵を索引により識別可能に記憶する記憶手段より読み出して、使用する暗号化鍵として登録する手段を実現させるためのコンピュータプログラム。

【請求項１５】　端末とアクセスポイントとを無線通信により接続する無線通信システムの制御方法であって、
前記アクセスポイントにおいて使用するものと決定された暗号化鍵の索引を、暗号化鍵を索引により識別可能に記憶する記憶手段より読み出して、使用する暗号化鍵として登録する工程と前記アクセスポイントにおいて使用するものと決定された暗号化鍵の索引を前記端末に配信する配信工程と、
前記端末において、前記アクセスポイントより配信された索引により識別される暗号化鍵を、暗号化鍵を索引により識別可能に記憶する記憶手段より読み出して、使用する暗号化鍵として登録する工程とを備えることを特徴とする無線通信システムの制御方法。

【請求項１６】　有線通信網に接続されたアクセスポイントとを含む無線通信システムであって、
前記クライアント端末および前記アクセスポイントの双方の機器に装着された記憶媒体と、
前記記憶媒体内にデータ暗号化用の鍵情報をインデックッス番号と対応付けて記憶する手段と、
前記機器側からの前記インデックッス番号による問合せに対応して、前記記憶媒体から前記暗号化用の鍵情報を返送する手段とを有することを特徴とする無線通信システム。

【請求項１７】　前記記憶媒体より読み出した前記暗号化用の鍵を用いて通信データを暗号化する暗号化手段を更に有することを特徴とする請求項１６記載の無線通信システム。

【請求項１８】　前記暗号化手段は、通信フレーム上の

全てのデータを暗号化の対象とすることを特徴とする請求項１７記載の無線通信システム。

【請求項１９】　前記暗号化手段は、通信フレーム上のマネジメントデータを除いたデータを暗号化の対象とすることを特徴とする請求項１７記載の無線通信システム。

【請求項２０】　前記アクセスポイントは、当該アクセスポイントが現在利用中の暗号化鍵情報のインデックス番号が付加されたビーコンフレームを一定時間間隔で放送送信して、前記アクセスポイントが統括するエリアのプロファイル情報を前記クライアント端末に通知することを特徴とする請求項１６乃至１９のいずれか１項に記載の無線通信システム。

【請求項２１】　前記無線ローカル通信網において、前記アクセスポイントは、前記インデックッス用番号の範囲内で前記鍵情報を所定間隔で変更する手段を有し、乱数に対応した前記暗号化用の鍵情報を前記着脱可能な記憶媒体より読み出し、当該暗号化鍵情報を用いて前記アクセスポイントから送信されるデータを暗号化することを特徴とする請求項１７乃至２０のいずれかに記載の無線通信システム。

【請求項２２】　前記アクセスポイントは、当該アクセスポイントークライアント端末間でのローカル通信に用いる暗号化データ量を計測する手段と、ローカル通信の有無を確認する手段とを有し、前記暗号化データ量が規定された量を越えた都度、１通信フレーム単位のローカル通信の終了後、暗号化鍵の変更処理を行い以降のローカル通信に利用する暗号化鍵を前記手段で変更することを特徴とする請求項２１記載の無線通信システム。

【請求項２３】　前記アクセスポイントは、当該アクセスポイントークライアント端末間でのローカル通信に用いられる通信時間を計時する手段と、ローカル通信の有無を確認する手段とを有し、前記暗号化通信時間が規定された時間を経過する都度、１通信フレーム単位のローカル通信の終了後、暗号化鍵の変更処理を行い以降のローカル通信に利用する暗号化鍵を前記手段で変更することを特徴とする請求項２１記載の無線通信システム。

【請求項２４】　前記暗号化鍵の変更に従って、前記アクセスポイントは、前記ビーコンフレームを用いて通知される暗号化鍵のインデックス番号が前記アクセスポイントが利用中の暗号化鍵に追随して変化させることを特徴とする請求項２２または２３に記載の無線通信システム。

【請求項２５】　前記ビーコンフレーム上に、トラブル発生を通知するための警告情報を付加して送信する手段を有し、前記アクセスポイントが、前記暗号化用の鍵情報を前記着脱可能な記憶媒体より読み出しに失敗場合、前記クライアント端末に対して暗号化鍵の定常的な変更に失敗した旨を、前記ビーコンフレームを用いて通知することを特徴とする請求項２１乃至２４のいずれか記載の無線通信システム。

【請求項２６】　前記クライアント端末は、受信したビーコンフレーム上の利用暗号化鍵のインデックス番号を読み出す手段を有し、当該インデックス番号の変更に応じて、前記記憶媒体からデータ暗号化用の鍵情報を入手し、通信データの暗号化を行うことを特徴とする請求項２４記載の無線通信システム。

【請求項２７】　前記クライアント端末は、受信したビーコンフレーム上の暗号化の定常的な変更に失敗した旨の情報を読み出す手段と、当該クライアント端末利用者に対して警告表示を行う手段とを有し、前記失敗を検出した際には前記端末利用者に対して警告表示を行うことを特徴とする請求項２５記載の無線通信システム。

【請求項２８】　無線通信媒体が無線ＬＡＮであることを特徴とする請求項１６乃至２７のいずれかに記載の無線通信システム。

【請求項２９】　無線通信媒体が構内ＰＨＳであることを特徴とする請求項１６乃至２７のいずれかに記載の無線通信システム。

【請求項３０】　無線通信媒体がブルートゥースであることを特徴とする請求項１６乃至２７のいずれかに記載の無線通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば無線通信媒体を用いたローカル通信ネットワーク等において、暗号化通信を行う通信システム及び暗号化方法に関するもので、特に、通信データの暗号化に利用する暗号化鍵の自律的な変更を用いて無線通信傍受者に対するセキュリティを強化する無線通信システムおよびその制御方法に関するものである。

【０００２】

【従来の技術】従来の無線ＬＡＮシステム等の無線ローカル通信システムには、ピアツーピア接続された無線端末のみで構成されるインデペンデント方式のものや、ひとつのアクセスポイントと無線端末とでサービスエリア（基本サービスセット）を構成し、複数のアクセスポイント同士を有線接続して接続して構成されるインフラストラクチャ方式のものがある。後者の方式によるシステムは、無線通信機能を備えたパーソナルコンピュータ等のクライアント端末と、クライアント端末から有線ＬＡＮに接続するための無線通信機能を有するアクセスポイントを備えている。このようなシステムにおいては、クライアント端末間は無線で、有線ＬＡＮに対してはアクセスポイント経由で通信を行う。無線通信では通信内容を傍受可能であるために、情報の秘匿のためには暗号化通信を行う必要がある。そのために当該無線通信の基本サービスセットにて利用する暗号化鍵情報はひとつのサービスセットにおいては共有されていなければならない。サービスセットで使用される暗号化鍵情報は、通信

システムを構成するクライアント端末機器およびアクセスポイントの各々の初期設定処理段階で設定していた。

【０００３】

【発明が解決しようとする課題】しかしながら上記の従来例では、暗号化通信を傍受し、傍受した暗号化信号から無線ローカル通信システムの傍受した通信エリアで利用されている暗号化鍵を推定することが可能である。特に近年では、パーソナルコンピュータ等の情報処理機器の処理能力が向上し、一般に普及した安価な機器を用いて、傍受した暗号化信号から暗号化鍵を推定することが比較的短時間で行えるようになりつつある。そのため、無線ローカル通信システムの初期設定処理後、暗号化鍵の再設定を行わずに同一の暗号化鍵を用いて暗号化データ通信を継続していると、傍受者が暗号化鍵を特定した後でもその暗号化鍵を用いて通信を継続していることとなり、傍受者により暗号化通信の内容が解読されてしまうという事態も生じ得る。

【０００４】本発明は上記従来例に鑑みて成されたもので、アクセスポイントの主導で当該アクセスポイントが統括する無線エリア内で利用される暗号化鍵を自律的に変更することを可能とし、さらに、無線回線を通じて伝達される暗号鍵関連情報を暗号化鍵と対応させたインデックス情報に限定することで、暗号鍵情報を有さないクライアント端末以外による暗号化鍵の入手を困難とし、情報安全性を向上させた無線通信システムおよびその制御方法を提供することを目的とする。

【０００５】さらに、暗号化鍵情報とインデックス番号との関連付けを着脱可能な記憶媒体に記憶させることで、アクセスを許容する端末とアクセスを許容しない端末とを視覚的に識別でき、情報安全性を向上させた無線通信システムおよびその制御方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】上記目的を達成するために、本発明は次のような構成から成る。

【０００７】端末とアクセスポイントとを無線通信により接続する無線通信システムであって、前記端末およびアクセスポイントそれぞれに備えられ、暗号化鍵を索引により識別可能に記憶する記憶手段と、前記アクセスポイントにおいて使用するものと決定された暗号化鍵の索引を前記端末に配信する配信手段と、前記端末において、前記アクセスポイントより配信された索引により識別される暗号化鍵を前記記憶手段より読み出して、使用する暗号化鍵として登録する手段とを備える。

【０００８】さらに好ましくは、前記記憶手段は、前記端末およびアクセスポイントに対して着脱自在な記憶媒体を含む。

【０００９】さらに好ましくは、前記アクセスポイントにおいては、前記アクセスポイントと端末との間で通信されるデータ量が一定値に達する毎に使用する暗号化鍵を新たに決定する。

【００１０】さらに好ましくは、前記アクセスポイントにおいては、一定時間経過する毎に使用する暗号化鍵を新たに決定する。

【００１１】あるいは本発明の他の側面は次のような構成から成る。

【００１２】端末と無線通信により接続された無線通信制御装置であって、暗号化鍵を索引により識別可能に記憶する記憶手段と、使用する暗号化鍵を決定する鍵決定手段と、決定された暗号化鍵を前記記憶手段より読み出して、使用する暗号化鍵として登録する手段と、前記決定された暗号化鍵の索引を前記端末に配信する配信手段とを備える。

【００１３】さらに好ましくは、前記記憶手段は、着脱自在な記憶媒体を含む。

【００１４】さらに好ましくは、前記鍵決定手段は、前記端末との間で通信されるデータ量が一定値に達する毎に使用する暗号化鍵を新たに決定する。

【００１５】さらに好ましくは、前記鍵決定手段は、一定時間経過する毎に使用する暗号化鍵を新たに決定する。

【００１６】あるいは本発明の他の側面は次のような構成から成る。

【００１７】無線通信制御装置と無線通信により接続された端末装置であって、暗号化鍵を索引により識別可能に記憶する記憶手段と、前記無線通信制御装置より配信された索引により識別される暗号化鍵を前記記憶手段より読み出して、使用する暗号化鍵として登録する手段とを備える。

【００１８】あるいは本発明の他の側面は次のような構成から成る。

【００１９】有線通信網に接続されたアクセスポイントとを含む無線通信システムであって、前記クライアント端末および前記アクセスポイントの双方の機器に装着された記憶媒体と、前記記憶媒体内にデータ暗号化用の鍵情報をインデックッス番号と対応付けて記憶する手段と、前記機器側からの前記インデックッス番号による問合せに対応して、前記記憶媒体から前記暗号化用の鍵情報を返送する手段とを有する。

【００２０】

【発明の実施の形態】［第一の実施形態］以下、本発明に係る無線ローカル通信の暗号化システムの実施の形態について、添付の書面を参照しつつ説明する。

【００２１】本実施形態における無線ローカル通信の暗号化システムでは、無線ＬＡＮ（ISO8802.11準拠システム）を無線ローカル通信媒体とし、着脱可能な記憶媒体としてＩＣカードを用いて、無線ＬＡＮのインフラストラクチャモードを利用し、無線通信媒体上で、規定量のデータの通信が行われる毎に、無線媒体で利用する暗号化用鍵を自動的に変更する。

7

【００２２】図１は本実施形態における無線ローカル通信システムを含むＬＡＮシステムの構成概念図である。図１はデータ通信を行っていない状態を示している。ＬＡＮシステム全体は、バックボーン通信網である有線通信網（有線ＬＡＮ）１０と、ローカル無線通信網である無線ＬＡＮシステム１１とを有する。無線ＬＡＮシステム１１は、アクセスポイント１００とクライアント端末１１０、１２０、１３０によって構成されている。アクセスポイント１００は、無線ＬＡＮと有線ＬＡＮとを接続するだけでなく、基本サービスセット内の端末およびアクセスポイントによって共有される情報を、サービスセットの各端末に報知する制御装置としての機能を有している。

【００２３】また、アクセスポイント１００及びクライアント端末１１０，１２０，１３０それぞれは、記憶媒体としてのＩＣカード１０１、１１１、１２１、１３１それぞれを着脱可能なＩＣカードアダプタを備えている。このＩＣカード１０１，１１１，１２１，１３１それぞれには、暗号化のために利用する暗号化鍵情報とその暗号化鍵情報を示すためのインデックス値が併せて記憶されている。暗号通信時には、アクセスポイント１００および暗号化通信を行うクライアント端末には、ＩＣカードが装着される。

【００２４】アクセスポイント１００は、インフラストラクチャモードにおいて、無線エリア内に在圏する全てのクライアント端末にエリアプロファイル情報を報知するためのビーコンフレーム１２を放送形式で一定時間間隔で間欠的に送信する。エリアプロファイル情報は、アクセスポイント１００が統括する無線エリア（基本サービスセット）のプロファイル（設定情報の集まり）を示す情報である。本実施形態では、ビーコンフレーム１２により送信されるエリアプロファイル情報に、アクセスポイント１００が利用中の暗号化（ISO8802.11のＷＥＰ方式に従った暗号化）用の鍵番号（鍵の値を示すためのインデックス値）を含めて間欠送信している。なお、ＷＥＰ方式とは、ISO8802.11のオプション機能で、ＭＡＣ層（ＭＡＣ：メディアアクセス制御）でデータを暗号化し、メディア認証コード用データを付けて、エラーや改ざんの有無をチェックする方式である。この暗号化に使用される鍵をＷＥＰ鍵と呼ぶ。

【００２５】図２は、本実施形態における無線ローカル通信の暗号化システムにおいてデータ通信中の様子を示す概念図である。フレーム２０、２１が、データ通信の際に利用される動的ＷＥＰ鍵更新方式による暗号化データ通信フレームである。なお、本実施形態においては、エリア内で規定量のデータ通信が行われる毎にＷＥＰ鍵を更新している。

【００２６】図１３に、本実施形態の無線ＬＡＮクライアント端末の無線ＬＡＮ機能部の機能ブロック図を示す。

8

【００２７】無線部１３０１は送受信を司る。ベースバンド処理部１３０２は信号の変復調を司る。ＭＡＣコントロール部１３０３はデータの符号化・復号化及びタイミング管理を司る。制御部１３０４は、フレームレベル以上の制御を司る。ＲＡＭ１３０５はワークエリア用のメモリ、ＲＯＭ１３０６は制御プログラムを格納するメモリである。ＩＣカードインタフェース部１３０７は、ＩＣカード１３０９にデータを書き込み、またＩＣカード１３０９からデータを読み出すための電気的機械的インターフェースを提供する。ＩＣカード１３０９には、ＷＥＰ鍵の情報要素と各情報要素選択用のインデックス値が関連付けられて内部に記憶（図６参照）されている。アプリケーションインタフェース部１３０８は、無線ＬＡＮ機能部を利用して通信を行うクライアント端末における他の構成部分とのインターフェースを提供する。

【００２８】図１４に、本実施形態の無線ＬＡＮアクセスポイントの機能ブロック図を示す。

【００２９】無線部１４０１は送受信を司る。ベースバンド処理部１４０２は信号の変復調を司る。ＭＡＣコントロール部１４０３はデータの符号化・復号化及びタイミング管理を司る。制御部１４０４はフレームレベル以上の制御を司る。ＲＡＭ１４０５はワークエリア用のメモリ、ＲＯＭ１４０６は制御プログラムを格納するメモリである。ＩＣカードインタフェース部１４０７は、ＩＣカード１４０９にデータを書き込み、またＩＣカード１４０９からデータを読み出すための電気的機械的インターフェースを提供する。ＩＣカード１４０９には、ＷＥＰ鍵の情報要素と各情報要素選択用のインデックス値が関連付けられて内部に記憶（図６参照）されている。有線ＬＡＮインターフェース部１４０８は、アクセスポイントと有線ＬＡＮとのインターフェースを提供する。

【００３０】図３に無線ＬＡＮ（ISO8802.11準拠システム）のビーコン信号のフォーマット例を示す。ビーコン信号は、インフラストラクチャモードにおいて、アクセスポイントから全てのクライアント端末にブロードキャストでエリアの情報を報知するために用いられる信号である。図３のフォーマットには、媒体アクセス制御（ＭＡＣ）層のフレームであることを示すＭＡＣヘッダ３０１やタイムスタンプ３０２、後述する２オクテットのケーパビリティ情報３０４等、規格により定められたフィールドが定義されている。

【００３１】図４は、図３のビーコン信号に含まれるケーパビリティ(capability)情報３０４の規格化された内容を示す図である。ビット５からビット１５までは予備ビットとなっている。

【００３２】図５に、本実施形態の無線ＬＡＮ（ISO8802.11準拠システム）におけるビーコン信号のケーパビリティ情報３０４を拡張したフォーマット例を示す。本実施形態では、ビーコンフレーム信号上に２オクテットで

9

構成されているケーパビリティ情報３０４にて、予備エリア４０６として使用方法が保留されている１１ビットのうち、ビット５からビット１０の６ビットを、アクセスポイントが利用中のＷＥＰ鍵に対応するインデックス値を基本サービスセット内のクライアント端末に周知するための暗号鍵番号５０６として定める。暗号鍵番号５０６により、６４種類のＷＥＰ鍵を指定することができる。さらに、予備エリア４０６のビット１１を、アクセスポイント側での運用上の不具合（ＩＣカードからＷＥＰ鍵情報が読み出せない等）が生じていることを通知するための警告ビット５０７と定める。残り４ビットを予備エリアとして留保している。

【００３３】図６は、本実施形態において無線ＬＡＮのＷＥＰ鍵情報のデータ長が４０ビットである場合に、ＩＣカード内にＷＥＰ鍵情報として格納されている鍵情報登録テーブルの例を示す。ＩＣカードには、暗号鍵番号５０６はＷＥＰ鍵に対応するインデックス値（１～６４）そ表し、暗号鍵番号に対応して、実際の４０ビットのＷＥＰ鍵情報６０１～６６４が記憶されている。そして、インデックス値の入力に対して、入力されたインデックス値に対応するＷＥＰ鍵情報を返送する機能をＩＣカードは有している。この機能は、ＩＣカードに内蔵されたプロセッサにより、これも内蔵されたメモリに格納されたプログラムを実行することで遂行される。

【００３４】図７および図８はＩＣカード内の論理ファイル構造の模式図である。このうち、図７は最上位ＤＦ７００～７２０の識別用のＩＤ（ＡＩＤ）をサービスベンダ毎に割当てる方式で実装した一例である。図８は、最上位ＤＦ８００～８２０の識別用のＩＤ（ＡＩＤ）をサービス種別毎に割当てる方式で実装した一例である。いずれにしても、図７および図８のEF KEYINFO７２００１および８２００１）内の記憶エリアに、図６に示す記憶形態で記憶されている。したがって、ＩＣカードは、インデックス値が入力された場合、この論理ファイル構造をたどって鍵情報登録テーブルを参照し、入力されたインデックス値に対応するＷＥＰ鍵情報を獲得して出力することができる。

【００３５】＜ＷＥＰ鍵の変更手順＞無線ＬＡＮシステムにおけるＷＥＰ鍵の変更方法を、図９のシーケンスチャートおよび図１０のアクセスポイントの処理フローチャートと図１１のクライアント端末の処理フローチャートを用いて説明する。本実施形態では、無線アクセスポイントを介して通信されるデータ量が規定量を超過したことをＷＥＰ鍵変更のトリガとして利用する例を示す。アクセスポイント１００は、サービスエリア内のクライアント端末との間の通信データ量を、データの送受信が発生する都度カウンタ等を用いて積算し、あらかじめ定められた規定量と比較する。なおデータ量はデータ送信または受信に限って行うようにすることもできる。

【００３６】そして、図９に示すように、無線アクセスポイント１００が、それを介して通信されるデータ量が規定量を超過したと判定した場合には、当該無線アクセスポイントでは、図１０に示す処理が起動される。

10

【００３７】まず、現在までに積算した伝送データ量をカウントするカウンタをクリアし（１００１）、所定の演算により、変更する暗号鍵番号（ＷＥＰ鍵に対応するインデックス値）を選択する（１００２）。インデックス値を決定するための演算としては、たとえば最も簡単には直前の鍵番号に１を加算する方法や乱数を発生してその６４を法とする剰余をインデックスとする方法などが考えられる。重要な点は、直前の鍵番号が再度選択されないようにすることにある。また、仮に再度の選択を許すにしても、暗号通信文から暗号化鍵を推定するために必要な時間に対して十分短い間隔で暗号化鍵が変更されるように、鍵番号が決定される必要がある。鍵変更のトリガとなる通信データ量（以下、トリガデータ量と呼ぶ）もこの観点から決定されている必要がある。

【００３８】暗号鍵番号が決定されたなら、アクセスポイント１００は、装着されているＩＣカード１０１に対して、暗号鍵番号を付加したＷＥＰ鍵情報要求を発行する（１００３）。ＷＥＰ鍵情報要求を受信したＩＣカード１０１により、指定された暗号鍵番号に対するＷＥＰ暗号鍵情報を付加したＷＥＰ鍵情報応答が返送される。

【００３９】アクセスポイント１００がＷＥＰ暗号鍵情報応答を正常に受付けた場合（１００４－Ｙ）、現在データ通信中であるかの判定を行う（１００５）。データ通信中であれば、１データ通信単位に、終了まで待ち合わせを行う。データ通信中でなければ、今後利用する暗号化鍵（ＷＥＰの鍵）を前記ＩＣカードより受取ったＷＥＰ暗号鍵情報に変更し、警告表示用の警告ビットをクリアする（ステップ１００６）。そして、ビーコンフレームのケーパビリティ情報に、新たな暗号鍵番号（前記ＷＥＰ鍵に対応するインデックス値）および警告ビットをセットし、エリア内のクライアント端末に対してブロードキャストで通知する（ステップ１００７）。

【００４０】一方、例えばタイムアウトなどを生じて応答を正常に受付けられなかった場合（１００４－Ｎ）、警告表示用の警告ビットをセットし（１００８）、暗号鍵番号（前記ＷＥＰ鍵に対応するインデックス値）および警告ビット値をビーコンフレームのケーパビリティ情報にセットし、エリア内のクライアント端末に対してブロードキャストで通知する（ステップ１００７）。この場合、新たな暗号鍵番号は得られていないので、例えば現在の値をそのままセットすればよい。なお、データ量が規定値に達していない場合に送信されるビーコンフレームについては、暗号鍵情報５０６としては、使用されている暗号鍵番号をそのままセットすればよい。あるいは、例えば暗号鍵番号０により暗号鍵の変更がない旨を表示させる等により、暗号鍵番号が変更されていないことを示すこともできる。

【００４１】次に、ビーコンフレームを受信したクライアント端末１１０の動作を図１１を参照して説明する。なおいずれのクライアント端末も同様の動作を行う。

【００４２】クライアント端末１１０は、受信したビーコンフレームよりケーパビリティ情報内の「暗号鍵番号」５０６および「警告ビット」５０７を読み出し（１１０１）、警告ビットがセットされているか判定する（１１０２）。セットされていれば、クライアント端末において鍵が更新されなかった旨の警告表示を行って（１１０７）、１処理単位を終了する。一方、警告ビットがセットされていなければ、「暗号鍵番号」を参照し（１１０３）、変更が検出されなければ、そのまま１処理単位を終了する。

【００４３】「暗号鍵番号」の変更が検出された場合（１１０３）、クライアント端末１０１は、装着されているＩＣカード１１１に対して、暗号鍵番号を付加してＷＥＰ鍵情報要求を行う（１１０４）。ＩＣカード１１１は、指定された暗号鍵番号をＷＥＰ鍵情報に対応するインデックス値として、暗号鍵情報（ＷＥＰ暗号鍵情報）を付加してＷＥＰ鍵情報応答を返送する。

【００４４】クライアント端末１０１は、ＷＥＰ鍵情報応答を正常に受付けたか判定し（１１０５）、正常に受信したなら今後利用する暗号化鍵（ＷＥＰの鍵）をＩＣカード１１１より受取ったＷＥＰ暗号鍵情報に変更する。

【００４５】一方ＩＣカード１１１からのＷＥＰ鍵情報応答を正常に受付けられなかった場合（１１０５－Ｎ）、クライアント端末１０１に警告表示を行い（１１０７）、１処理単位を終了する。

【００４６】以上のアクセスポイントおよびクライアント端末およびそれぞれに接続されたＩＣカードの動作を図９に示している。図９においては、アクセスポイントはビーコン信号をサービスセット内のクライアント端末に対して定期的に送信（放送送信）している。そして、ビーコン信号９０１送信後に、最後にＷＥＰ鍵を変更してからの通信データ量が一定値を越えたなら、それをＷＥＰ鍵変更トリガ９０２として新たな暗号鍵番号を決定し、アクセスポイントに接続されたＩＣカードに対してＷＥＰ鍵情報要求９０３を発行して暗号鍵番号を通知し、それに対するＷＥＰ鍵情報応答９０４の受信を待つ。ＷＥＰ鍵情報応答９０４を受信したなら、そのＷＥＰ鍵情報応答に含まれるＷＥＰ鍵情報を新たな暗号鍵として使用すべく設定し、ビーコン信号９０５の暗号鍵番号フィールドに新たに決定された暗号鍵番号を設定してビーコン信号９０５を放送送信する。クライアント端末ではビーコン信号を受信すると、そこに含まれる信号に応じた設定を行うが、特に、暗号鍵番号に変更があると、クライアント端末に接続されたＩＣカードに対してＷＥＰ鍵情報要求９０７を発行して暗号鍵番号を通知し、それに対するＷＥＰ鍵情報応答９０８の受信を待つ。ＷＥＰ鍵情報応答９０８を受信したなら、そのＷＥＰ鍵情報応答に含まれるＷＥＰ鍵情報を新たな暗号鍵として使用すべくクライアント端末を設定する。

【００４７】以上の処理により、無線ＬＡＮ媒体上の通信データ量の既定値超過をトリガとして、暗号化用の鍵（ＷＥＰ暗号鍵）を、ネットワークの運用中に、自律的に更新することが可能となる。このため、当該サービスセット用ＩＣカードを保持しない無線ＬＡＮクライアント等の第三者による通信傍受に対するセキュリティを向上させることが可能となる。また、同時に権限なき第三者によるネットワークへのアクセスについてのセキュリティ向上も可能となる。

【００４８】特に、アクセスポイントから各端末への鍵情報の配信は、暗号鍵番号の配信という形で行われ、ＷＥＰ鍵情報そのものが配信されることはない。そのため、本実施形態において鍵管理に使用しているＩＣカードを保有していない端末においては、鍵情報そのものの配信を傍受して鍵を特定することが不可能となり、一層のセキュリティの向上を図ることができる。

【００４９】また、暗号鍵番号をビーコン信号に含ませて配信することで、鍵配信のための特別な手順が不要となり、セキュリティを確保しつつＷＥＰ鍵の変更を簡便迅速に行うことが可能となる。

【００５０】さらに、鍵情報をＩＣカードにより管理しているために、ＩＣカードそのものを新たな鍵情報を保持したＩＣカードに交換することで、一層セキュリティを向上させることができる。

【００５１】さらに、本実施形態では、ＷＥＰ鍵を変更する間隔を通信データ量により設定しておけるために、データの交換が頻繁なサービスセットにおいては頻繁にＷＥＰ鍵を変更することができる。

【００５２】［第二の実施形態］図１２に、無線アクセスポイントにて計時される“同一ＷＥＰ鍵継続時間タイマ”のタイムアップを、ＷＥＰ鍵変更のトリガ（図９の９０２）として利用する例を示す。

【００５３】無線アクセスポイント１００にて“同一ＷＥＰ鍵継続時間タイマ”がタイムアップした際、当該無線アクセスポイントでは、図１２に示す処理が起動される。

【００５４】まず、現在までの“同一ＷＥＰ鍵継続時間タイマ”を初期化（１２０１）した後、所定の演算により、変更する暗号鍵番号（ＷＥＰ鍵に対応するインデックス値）の選択を行う（１２０２）。同一ＷＥＰ鍵継続時間タイマは、図１４の制御部１４０４が備えるタイマを利用して実現できる。また、タイマは初期化後ただちに再スタートされる。

【００５５】アクセスポイント１００は、装着されているＩＣカード１０１に対して、暗号鍵番号（ＷＥＰ鍵に対応するインデックス値）を付加したＷＥＰ鍵情報要求を発行する（１２０３、９０３）。

13

【００５６】ＩＣカード１００は、指定された暗号鍵番号（ＷＥＰ鍵に対応するインデックス値）に対する、暗号鍵情報（ＷＥＰ鍵の情報）を付加したＷＥＰ鍵情報応答をアクセスポイント１００に返送する（９０４）。

【００５７】アクセスポイント１００が、ＷＥＰ鍵情報応答を正常に受付けた場合（１２０４－Ｙ）、現在データ通信中であるかの判定を行い（１２０５）、データ通信中であれば、１データ通信単位に終了まで待ち合わせを行い、データ通信中でなければ、今後利用する暗号化鍵（ＷＥＰの鍵）をＩＣカード１０１より受取った暗号鍵情報に変更し、警告表示用の警告ビットをクリアする（１２０６）。

【００５８】一方、ＷＥＰ鍵情報応答を正常に受付けられなかった場合（１２０４－Ｎ）、警告表示用の警告ビットをセットし（１２０８）、対応情報である鍵番号番号（ＷＥＰ鍵に対応するインデックス値）、警告ビット値を前記ビーコンフレームにセットし、エリア内のクライアント端末に対してブロードキャストで通知する（９０５、１２０７）。

【００５９】以上の処理により、本実施形態に示した制御を行うアクセスポイントと、第１の実施形態で示したクライアント端末の組み合わせにる無線ＬＡＮシステムにおいても、アクセスポイント１００にて計時される“同一ＷＥＰ鍵継続時間タイマ”のタイムアップをトリガとすることで、暗号化用の鍵（ＷＥＰ鍵）を実運用中に、自律的に更新することが可能となり、第一の実施形態と同様に、当該サービスセット用ＩＣカードを保持しない無線ＬＡＮクライアントといった第三者の傍受に対する通信セキュリティを向上させることが可能となる。

【００６０】また、同一ＷＥＰ鍵継続時間をプログラム可能としておけば、暗号鍵解読方法の洗練や暗号鍵解読に使用される処理装置の性能向上に応じて、同一ＷＥＰ鍵継続時間を短縮していくことで、セキュリティを維持することができる。

【００６１】また、鍵自体を配信せず、鍵番号を配信することにより簡便かつ迅速なＷＥＰ鍵の変更を行えることから、鍵を変更する間隔を短時間に設定しても、それに起因する処理処理遅延を抑制できる。そのため、鍵変更の頻度を高めてセキュリティ破りに対する耐性を向上させることができる。

【００６２】さらに、本実施形態では、ＷＥＰ鍵を変更する間隔を時間により設定しておけるために、一定時間毎の鍵の変更を保証することができる。（他の実施形態）前記実施形態においては、ローカル無線通信システム用の無線媒体として、ISO8802.11準拠の無線ＬＡＮシステムのインフラストラクチャモードを利用した場合の無線通信回線上で伝送されるデータを暗号化するための暗号鍵を定期的に変更する例を示した。しかし、ISO8802.11準拠の無線ＬＡＮシステムのインフラストラクチャモード以外でも、１つのアクセスポイントと複数のクライアントから構成され、アクセスポイントから当該無線エリアに関する情報が定常的に報知されるローカル無線通信システム、例えば構内ＰＨＳやブルートゥース(Blue tooth)等への応用が可能である。

14

【００６３】また、前記実施形態においては、暗号化鍵（ＷＥＰ鍵）情報格納モジュールとしてＩＣカードを利用しているが、ＰＣカード等の他の記憶モジュールを用いても同様の効果が得られる。

【００６４】また、上記実施形態では、鍵の管理はＩＣカードにより行われているが、アクセスポイントおよび各クライアント端末それぞれが鍵の管理を行う構成であってもよい。この場合には、アクセスポイントから各端末に対してＷＥＰ鍵を送信するシーケンスを付加することで更にセキュリティを向上させることができる。

【００６５】また、第１実施形態においてＷＥＰ鍵変更のトリガとなるデータ量は、暗号化の対象となるデータ量であってもよいし、送受信されたデータ全体のデータ量であってもよい。

【００６６】なお、本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用してもよい。

【００６７】また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（または記録媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても達成される。

【００６８】この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコード自体およびプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【００６９】また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム(OS)などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

【００７０】さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

【００７１】
【発明の効果】以上説明したように、本発明によれば、無線ローカル通信システムにおいて、アクセスポイントの主導で当該アクセスポイントが統括する無線エリア内で利用する暗号化鍵を自律的に変更することが可能となる。また、無線回線を通じて伝達される暗号鍵関連情報を、端末に接続された記憶媒体アクセスのためのインデックス情報に限定しているため、当該暗号鍵情報記憶済みの記憶媒体を持つクライアント端末以外では、実際の暗号化鍵情報を入手することが困難となる。このため、無線ローカル通信システムでのデータ通信における情報セキュリティの向上に繋がる。
【００７２】また、暗号化鍵情報とインデックス番号の関連付けを着脱可能な記憶媒体に記憶させているため、クライアント端末機器のアクセス可否を記憶媒体の装着状態によって視覚的に識別させることが可能となる。
【００７３】さらに、暗号化鍵情報とインデックス番号の関連付けを着脱可能な記憶媒体に記憶させているため、権限なき第三者によるネットワークへのアクセスについてのセキュリティの向上が可能となる。
【００７４】さらに、暗号鍵番号を特別な手順無しで各端末に配信することができるために、セキュリティを確保しつつ鍵の変更を簡便迅速に行うことが可能となる。
【００７５】さらに、鍵情報を着脱自在な記憶媒体により管理しているために、記憶媒体そのものを新たな鍵情報を保持した記憶媒体に交換することで、一層セキュリティを向上させることができる。
【００７６】さらに、鍵を変更する間隔を通信データ量により設定しておけるために、データの交換が頻繁なサービスセットにおいては頻繁に鍵を変更することができる。
【００７７】また、鍵を変更する時間間隔を変更可能としておけば、鍵解読方法の洗練や鍵解読に使用される処理装置の性能向上に応じて、その時間間隔を短縮していくことで、セキュリティを維持することができる。
【００７８】また、鍵自体を配信せず、鍵番号を配信することにより簡便かつ迅速な鍵の変更を行えることから、鍵を変更する間隔を短時間に設定しても、それに起因する処理処理遅延を抑制できる。そのため、鍵変更の頻度を高めてセキュリティ破りに対する耐性を向上させることができる。
【００７９】さらに、鍵を変更する間隔を時間により設定しておくことで、一定時間毎の鍵の変更を保証することができる。
【図面の簡単な説明】
【図１】実施形態における無線ローカル通信の暗号化方式システムの構成概念図
【図２】実施形態における無線ローカル通信の暗号化方式システムの構成概念図
【図３】ISO8802．11準拠システムのビーコンフレームフォーマットの図
【図４】ISO8802．11準拠システムのビーコンフレーム上ケーパビリティ情報フォーマットの図
【図５】実施形態におけるケーパビリティ情報のフォーマットの拡張例の図
【図６】実施形態のＷＥＰ鍵情報要素登録テーブル例の図
【図７】実施形態のＩＣカード上の論理フォーマット構成例１の図
【図８】実施形態のＩＣカード上の論理フォーマット構成例２の図
【図９】実施形態ＬＡＮシステムのＷＥＰ鍵の変更シーケンスチャート例の図
【図１０】第１の実施形態の無線ＬＡＮアクセスポイントのＷＥＰ鍵変更フローチャート
【図１１】実施形態の無線ＬＡＮクライアント端末のＷＥＰ鍵変更フローチャート
【図１２】第２の実施形態の無線ＬＡＮアクセスポイントのＷＥＰ鍵変更フローチャート
【図１３】実施形態の無線ＬＡＮクライアント端末の機能ブロック図
【図１４】実施形態の無線ＬＡＮアクセスポイントの機能ブロック図
【符号の説明】
１０　有線通信網（有線ＬＡＮ）
１１　ローカル無線通信網（無線ＬＡＮ）
１２　ビーコンフレーム
２０　動的ＷＥＰ鍵によって暗号化されたデータフレーム
２１　動的ＷＥＰ鍵によって暗号化されたデータフレーム
１００　アクセスポイント
１０１　ＩＣカード（ＷＥＰ鍵テーブル格納）
１１０　クライアント端末
１１１　ＩＣカード（ＷＥＰ鍵テーブル格納）
１２０　クライアント端末
１２１　ＩＣカード（ＷＥＰ鍵テーブル格納）
１３０　クライアント端末
１３１　ＩＣカード（ＷＥＰ鍵テーブル格納）
１３０１　無線部
１３０２　ベースバンド部
１３０３　ＭＡＣコントロール部
１３０４　制御部
１３０５　ＲＡＭ
１３０６　ＲＯＭ
１３０７　ＩＣカードインタフェース部
１３０８　アプリケーションインタフェース部
１３０９　ＩＣカード
１４０１　無線部
１４０２　ベースバンド部

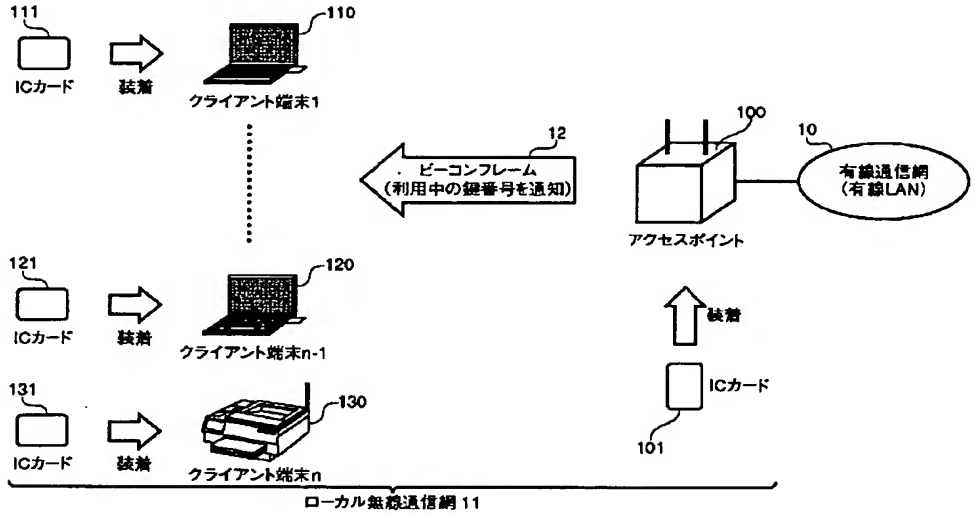
17

１４０３　ＭＡＣコントロール部
１４０４　制御部
１４０５　ＲＡＭ
１４０６　ＲＯＭ

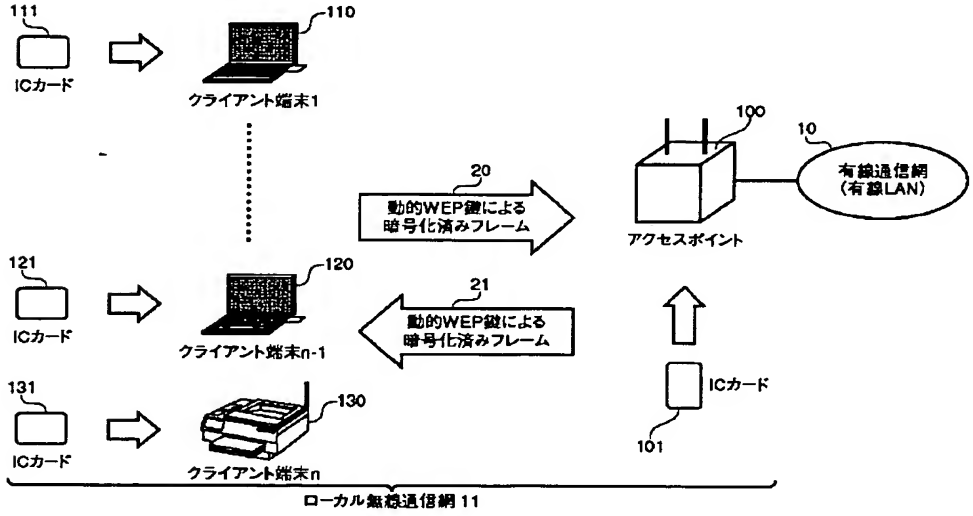
18

１４０７　ＩＣカードインタフェース部
１４０８　有線ＬＡＮ（通信網）インタフェース部
１４０９　ＩＣカード

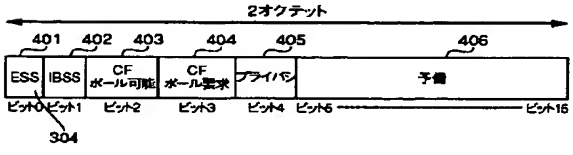
【図１】



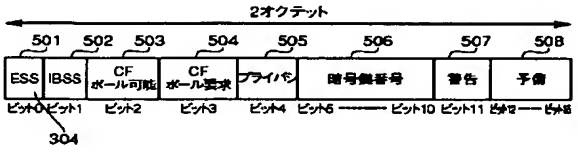
【図２】



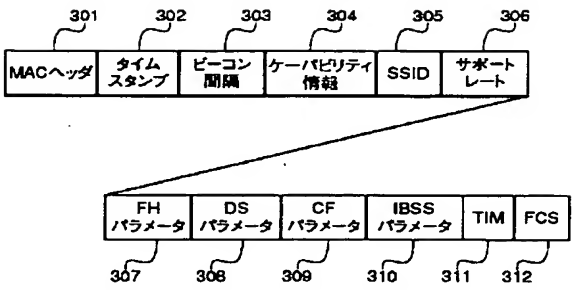
【図４】



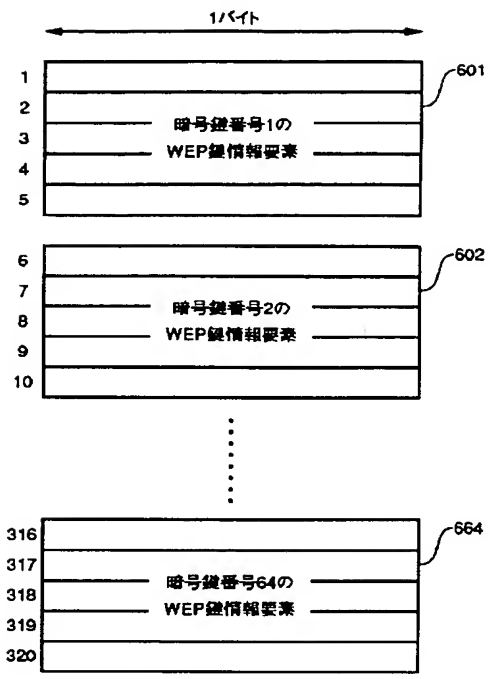
【図５】



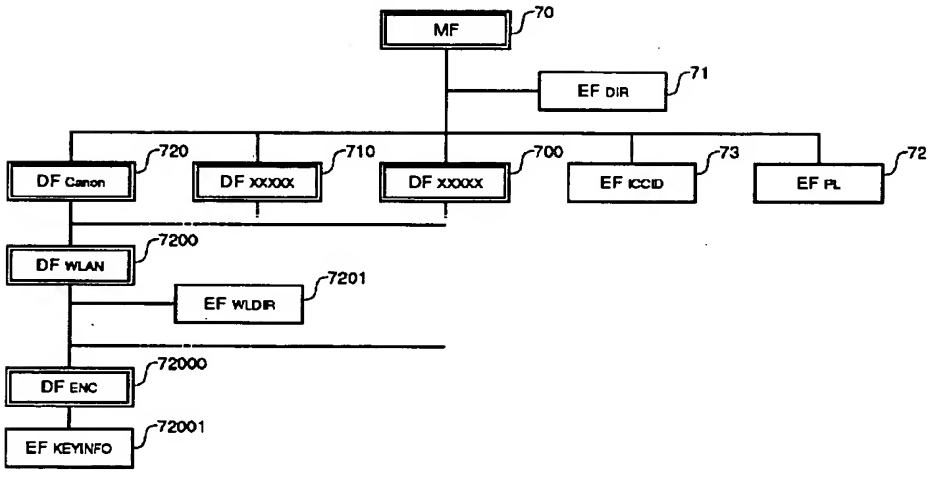
【図３】


301
302
303
304
305
306
MACヘッダ
タイムスタンプ
ビーコン間隔
ケーパビリティ情報
SSID
サポートレート
FH パラメータ
DS パラメータ
CF パラメータ
IBSS パラメータ
TIM
FCS
307
308
309
310
311
312

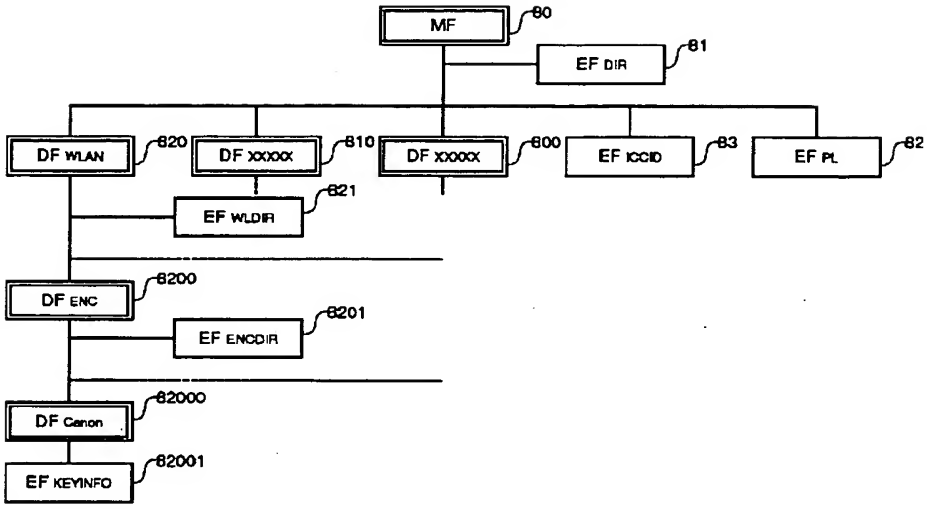
【図６】


1バイト
1
2
3
4
5
601
暗号鍵番号1の
WEP鍵情報要素
6
7
8
9
10
602
暗号鍵番号2の
WEP鍵情報要素
316
317
318
319
320
664
暗号鍵番号64の
WEP鍵情報要素

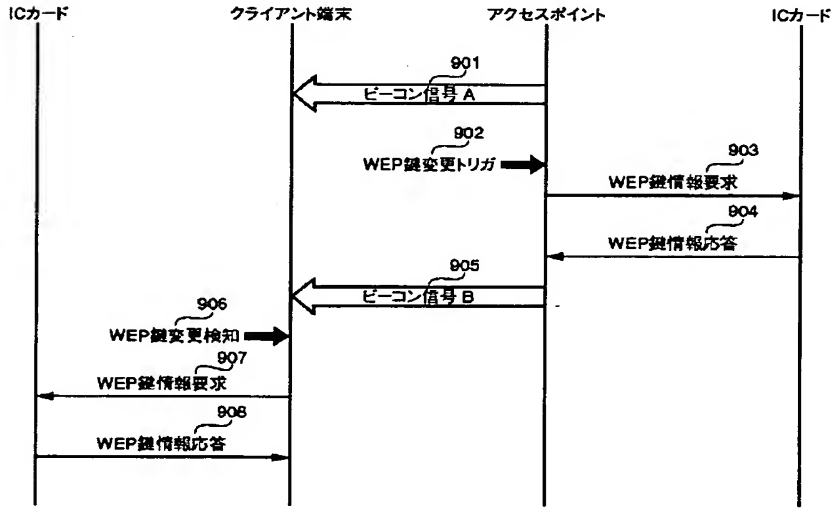
【図７】


MF
70
EF DIR
71
DF Canon
720
DF XXXX
710
DF XXXX
700
EF ICCID
73
EF PL
72
DF WLAN
7200
EF WLDIR
7201
DF ENC
72000
EF KEYINFO
72001

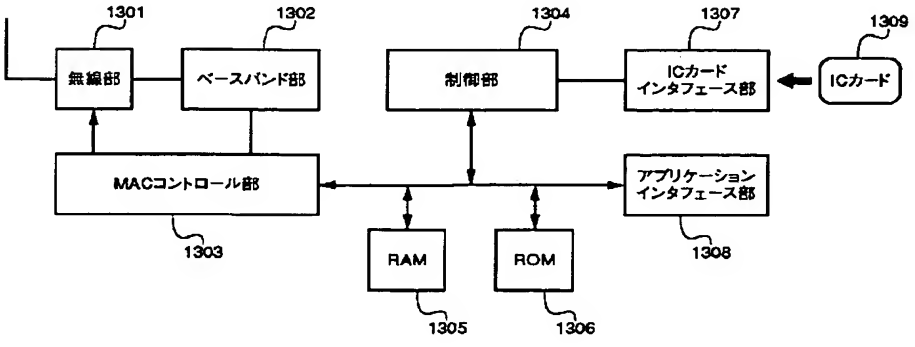
【図８】


MF
60
EF DIR
61
DF WLAN
820
DF XXXX
810
DF XXXX
800
EF ICCID
83
EF PL
82
EF WLDIR
821
DF ENC
8200
EF ENCDIR
8201
DF Canon
82000
EF KEYINFO
82001

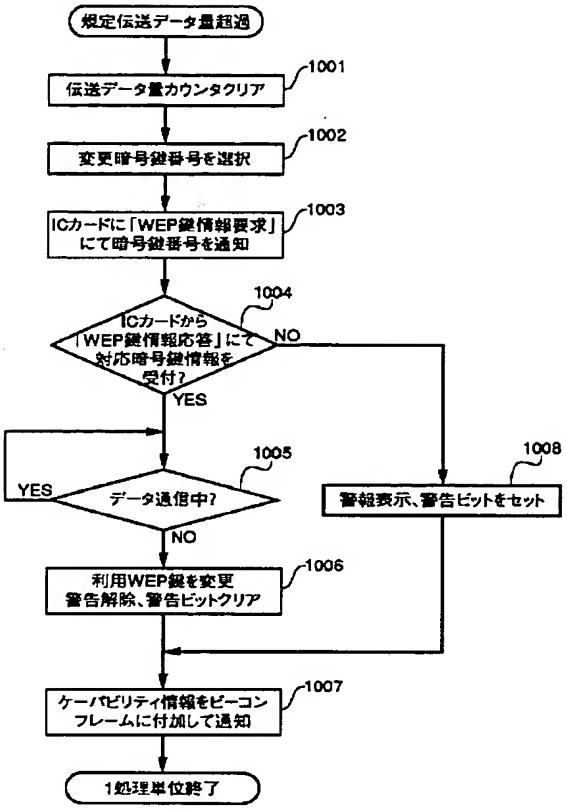
【図９】


ICカード
クライアント端末
アクセスポイント
ICカード
901
ビーコン信号 A
902
WEP鍵変更トリガ
903
WEP鍵情報要求
904
WEP鍵情報応答
905
ビーコン信号 B
906
WEP鍵変更検知
907
WEP鍵情報要求
908
WEP鍵情報応答

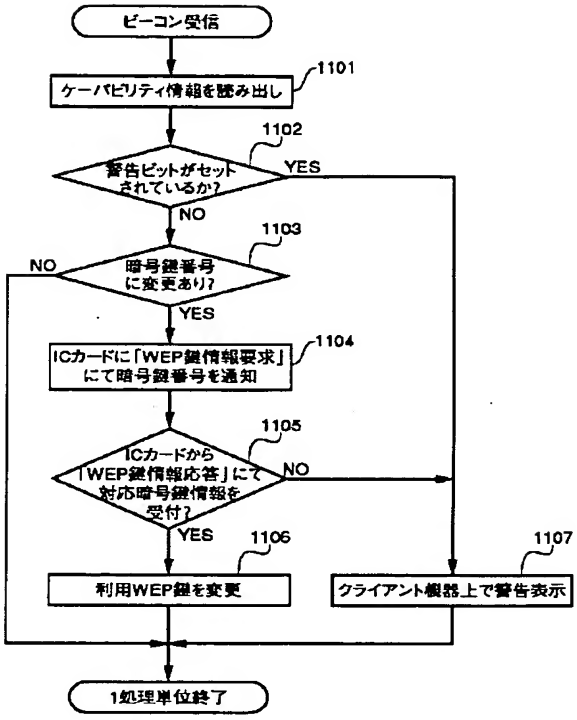
【図１３】


1301
無線部
1302
ベースバンド部
1304
制御部
1307
ICカード
インタフェース部
1309
ICカード
MACコントロール部
1303
アプリケーション
インタフェース部
1308
RAM
1305
ROM
1306

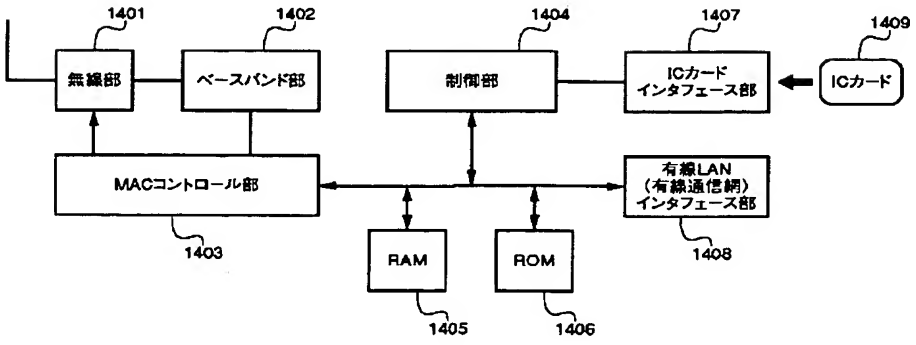
【図１０】


規定伝送データ量超過
伝送データ量カウンタクリア
1001
変更暗号鍵番号を選択
1002
ICカードに「WEP鍵情報要求」にて暗号鍵番号を通知
1003
ICカードから「WEP鍵情報応答」にて対応暗号鍵情報を受付?
1004
NO
YES
データ通信中?
1005
YES
NO
警報表示、警告ビットをセット
1008
利用WEP鍵を変更 警告解除、警告ビットクリア
1006
ケーパビリティ情報をビーコンフレームに付加して通知
1007
1処理単位終了

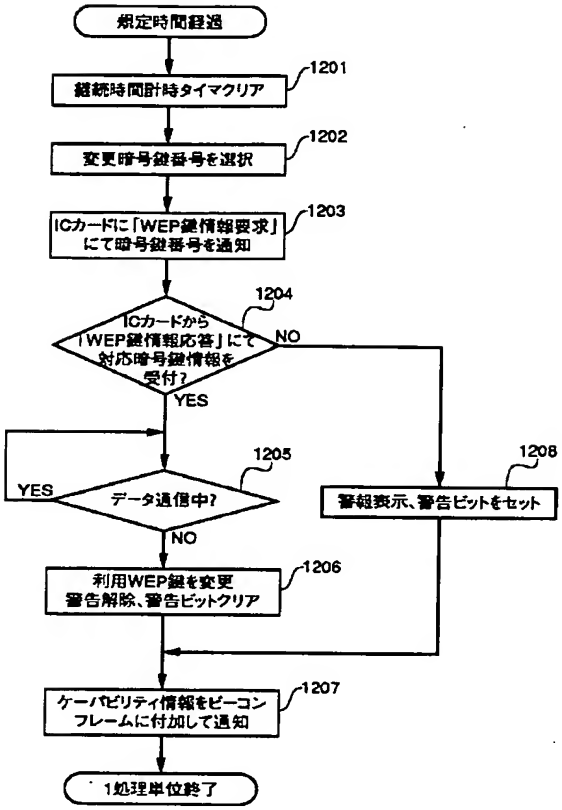
【図１１】


ビーコン受信
ケーパビリティ情報を読み出し
1101
警告ビットがセットされているか?
1102
YES
NO
暗号鍵番号に変更あり?
1103
NO
YES
ICカードに「WEP鍵情報要求」にて暗号鍵番号を通知
1104
ICカードから「WEP鍵情報応答」にて対応暗号鍵情報を受付?
1105
NO
YES
利用WEP鍵を変更
1106
クライアント機器上で警告表示
1107
1処理単位終了

【図１４】


1401
無線部
1402
ベースバンド部
1404
制御部
1407
ICカードインタフェース部
1409
ICカード
MACコントロール部
1403
有線LAN（有線通信網）インタフェース部
1408
RAM
1405
ROM
1406

【図１２】


規定時間経過
1201
継続時間計時タイマクリア
1202
変更暗号鍵番号を選択
1203
ICカードに「WEP鍵情報要求」にて暗号鍵番号を通知
1204
ICカードから「WEP鍵情報応答」にて対応暗号鍵情報を受付?
NO
YES
1205
YES
データ通信中?
NO
1208
警報表示、警告ビットをセット
1206
利用WEP鍵を変更
警告解除、警告ビットクリア
1207
ケーパビリティ情報をビーコンフレームに付加して通知
1処理単位終了